UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/824,162	04/14/2004	Scott A. Konersmann	MS307731.1/MSFTP623US	6351

27195 7590 08/23/2007

AMIN. TUROCY & CALVIN, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER	
JUNG, DAVID YIUK	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
08/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/824,162	KONERSMANN, SCOTT A.	
	Examiner	Art Unit	
	David Y. Jung	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) 1-22 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) 1-22 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 2004;2005;2007.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

CLAIMS PRESENTED

Claims 1-22 are presented.

NOTES ON ART

http://www.verisign.com/wss/WS-SecureConversation.pdf acknowledges Mr. Scott Konersmann (same name and same company as that of the inventor of this patent application)

CLAIM REJECTIONS

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Regarding claims 1-22, the claimed invention is directed to non-statutory subject matter. Claims recite only perfunctory recitation of functional material (computer readable medium, etc.). Aside from this, the claims recite only nonfunctional descriptive material. When nonfunctional descriptive material is recorded on some computer-readable medium, in a computer or on an electromagnetic carrier signal, it is not statutory since no requisite functionality is present to satisfy the practical application requirement. Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier

signal, does not make it statutory. See Diehr, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in Benson were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer."). Such a result would exalt form over substance.

For further guidance on the term "nonfunctional", please see MPEP 2106.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over and Helland (http://www.microsoft.com/presspass/exec/flessner/04-11flessnerteched.mspx) and Bresson (cited by Applicant, EMMANUEL BRESSON, et al., Provably Authenticated Group Diffie-Hellman Key Exchange, CCS'01, 2001, pp. 255-264, Philadelphia, Pennsylvania, USA) and Ietf (http://tools.ietf.org/html/draft-ietf-sip-rfc2543bis-09, section 26) and SecureConversation(http://www.verisign.com/wss/WS-SecureConversation.pdf).

Regarding claim 1, Bresson teaches A communication system comprising: a secure message generation system that employ a first [ ] to encrypt a first message to be sent to a second service; and, a secure message receiver system that employs a second [ ] to decrypt a second message received from the second service (Bresson, pages 255-256, i.e., encryption, decryption).

These passages of Bresson do not teach "dialog session" or "session key."

Ietf teaches "dialog session (Section 26.1.4 Tearing Down Session, the first paragraph, the discussion on dialog and/or session)" and "session key (Section 26.1.3 Tampering with Message Bodies, the third paragraph, the discussion on session key and on end-to-end security)" for the motivation of security.

These passages of Bresson and Ietf are not explicit about the particular way that the claimed invention, as a whole, would produce such autonomous nature of data handling. This is difficult to quote from any single phrase or any single word of the claim; the autonomous nature is difficult to quote, but prominently exists. For example, the dialog session key for encrypting a message and the dialog session key for decrypting that message or any other message can be different. Separate dialog keys permit separate fiefdoms instead of the entire kingdom of network being ruled by a single session key.

Helland teaches such autonomous nature. Mr. Helland (the person in this Helland reference) is of the same company as that of this patent application. Helland (the reference) contains a section in which Mr. Helland and Mr. Flessner discuss

fiefdom and autonomous nature (which are usually expressed in certificates and/or dialog sessions being unique).

These passage of Bresson, Ietf, Helland are not explicit about the different dialog keys being used for the same service (as in the claims).

SecureConversation teaches such different dialog keys being used for the same service (section 5. Deriving Keys, i.e., the derived key situation permits and recommends each party changing session keys and the other party being able to derive the keys needed for use in the service) for the motivation of establishing and sharing security contexts.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the teachings of Bresson, Ietf, Helland and SecureConversation for the motivations noted in the previous paragraphs so as to teach the claimed invention.

2. The communication system of claim 1, the secure message generation system comprising: a service pair encryption component that employs an initiator private key to encrypt authentication information; a key exchange key encryption component that employs a target public key to encrypt a key exchange key;

[Bresson, pages 255-256 teaches the key exchange key and the features using the key exchange key.]

a dialog session key encryption component that employs the key exchange key to encrypt the first dialog session key;

a message body encryption component that employs the first dialog session key to encrypt a message body of the first message to be sent to the second service;

[Ietf, Section 26.1 teaches dialog session key and the features using the dialog session key.]

and,

a message generator that provides the encrypted first message to the second service, the encrypted first message being based, at least in part, upon the encrypted authentication information, the encrypted key exchange key, the encrypted first dialog session key and the encrypted message body.

[Such message handling is implied in a communication. Messages are often used in communication.]

3. The communication system of claim 2, the key exchange key comprising a symmetric key.

Symmetric keys are well known in the art for the motivation of convenience in security (often easier generation and easier distribution).

4. The communication system of claim 2, the key exchange key comprising a 128-bit symmetric key.

Such application of symmetric keys are well known in the art for the motivation of convenience in security (often easier generation and easier distribution).

Regarding claims 6-12, such various policy handlings well known for security and efficiency.

Regarding claim 13, Bresson teaches A method facilitating secure communication comprising: providing an encrypted first message of a dialog based, at least in part, upon a first [ ] key; and, decrypting an encrypted second message of the dialog, decryption being based, at least in part, upon a second [ ] key(Bresson, pages 255-256, i.e., encryption, decryption).

These passages of Bresson do not teach "dialog session" or "session key."

Ietf teaches "dialog session (Section 26.1.4 Tearing Down Session, the first paragraph, the discussion on dialog and/or session)" and "session key (Section 26.1.3 Tampering with Message Bodies, the third paragraph, the discussion on session key and on end-to-end security)" for the motivation of security.

These passages of Bresson and Ietf are not explicit about the particular way that the claimed invention, as a whole, would produce such autonomous nature of data handling. This is difficult to quote from any single phrase or any single word of the claim; the autonomous nature is difficult to quote, but prominently exists. For example, the dialog session key for encrypting a message and the dialog session key for decrypting that message or any other message can be different. Separate dialog keys permit separate fiefdoms instead of the entire kingdom of network being ruled by a single session key.

Helland teaches such autonomous nature. Mr. Helland (the person in this Helland reference) is of the same company as that of this patent application. Helland

(the reference) contains a section in which Mr. Helland and Mr. Flessner discuss fiefdom and autonomous nature (which are usually expressed in certificates and/or dialog sessions being unique).

These passage of Bresson, Ietf, Helland are not explicit about the different dialog keys being used for the same service (as in the claims).

SecureConversation teaches such different dialog keys being used for the same service (section 5. Deriving Keys, i.e., the derived key situation permits and recommends each party changing session keys and the other party being able to derive the keys needed for use in the service) for the motivation of establishing and sharing security contexts.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the teachings of Bresson, Ietf, Helland and SecureConversation for the motivations noted in the previous paragraphs so as to teach the claimed invention.

. Regarding claims 14-19, such various policy handlings well known for security and efficiency.

On claim 20, Bresson teaches A data packet transmitted between two or more computer components that facilitates secure communication, the data packet comprising: a key exchange key header comprising an encrypted key exchange key; a [ ] key header comprising a first [ ] key encrypted with the key exchange key; and, a message body field comprising a message encrypted with the first [ ] key, the data packet received by a service that employs a second [ ] key to

encrypt a message the service originates(Bresson, pages 255-256, i.e., encryption, decryption).

These passages of Bresson do not teach "dialog session" or "session key."

Ietf teaches "dialog session (Section 26.1.4 Tearing Down Session, the first paragraph, the discussion on dialog and/or session)" and "session key (Section 26.1.3 Tampering with Message Bodies, the third paragraph, the discussion on session key and on end-to-end security)" for the motivation of security.

These passages of Bresson and Ietf are not explicit about the particular way that the claimed invention, as a whole, would produce such autonomous nature of data handling. This is difficult to quote from any single phrase or any single word of the claim; the autonomous nature is difficult to quote, but prominently exists. For example, the dialog session key for encrypting a message and the dialog session key for decrypting that message or any other message can be different. Separate dialog keys permit separate fiefdoms instead of the entire kingdom of network being ruled by a single session key.

Helland teaches such autonomous nature. Mr. Helland (the person in this Helland reference) is of the same company as that of this patent application. Helland (the reference) contains a section in which Mr. Helland and Mr. Flessner discuss fiefdom and autonomous nature (which are usually expressed in certificates and/or dialog sessions being unique).

These passage of Bresson, Ietf, Helland are not explicit about the different dialog keys being used for the same service (as in the claims).

SecureConversation teaches such different dialog keys being used for the same service (section 5. Deriving Keys, i.e., the derived key situation permits and recommends each party changing session keys and the other party being able to derive the keys needed for use in the service) for the motivation of establishing and sharing security contexts.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the teachings of Bresson, Ietf, Helland and SecureConversation for the motivations noted in the previous paragraphs so as to teach the claimed invention.

On claim 21, Bresson teaches A computer readable medium storing computer executable components of a communication system, comprising: a secure message generation system component that employs a first [ ] key to encrypt a first message to be sent to a second service; and.a secure message receiver system component that employs a second [ ] key to decrypt a second message received from the second service(Bresson, pages 255-256, i.e., encryption, decryption).

These passages of Bresson do not teach "dialog session" or "session key."

Ietf teaches "dialog session (Section 26.1.4 Tearing Down Session, the first paragraph, the discussion on dialog and/or session)" and "session key (Section 26.1.3 Tampering with Message Bodies, the third paragraph, the discussion on session key and on end-to-end security)" for the motivation of security.

These passages of Bresson and Ietf are not explicit about the particular way that the claimed invention, as a whole, would produce such autonomous nature of data

handling. This is difficult to quote from any single phrase or any single word of the claim; the autonomous nature is difficult to quote, but prominently exists. For example, the dialog session key for encrypting a message and the dialog session key for decrypting that message or any other message can be different. Separate dialog keys permit separate fiefdoms instead of the entire kingdom of network being ruled by a single session key.

Helland teaches such autonomous nature. Mr. Helland (the person in this Helland reference) is of the same company as that of this patent application. Helland (the reference) contains a section in which Mr. Helland and Mr. Flessner discuss fiefdom and autonomous nature (which are usually expressed in certificates and/or dialog sessions being unique).

These passage of Bresson, Ietf, Helland are not explicit about the different dialog keys being used for the same service (as in the claims).

SecureConversation teaches such different dialog keys being used for the same service (section 5. Deriving Keys, i.e., the derived key situation permits and recommends each party changing session keys and the other party being able to derive the keys needed for use in the service) for the motivation of establishing and sharing security contexts.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the teachings of Bresson, Ietf, Helland and SecureConversation for the motivations noted in the previous paragraphs so as to teach the claimed invention.

On claim 22, Bresson teaches A communication system comprising: means for generating a secure first message employing a first [ ] key to encrypt a first message to be sent to a second service; means for receiving a secure second message from the second service; and, means for decrypting the second message employing a second [ ] key(Bresson, pages 255-256, i.e., encryption, decryption).

These passages of Bresson do not teach "dialog session" or "session key."

Ietf teaches "dialog session (Section 26.1.4 Tearing Down Session, the first paragraph, the discussion on dialog and/or session)" and "session key (Section 26.1.3 Tampering with Message Bodies, the third paragraph, the discussion on session key and on end-to-end security)" for the motivation of security.

These passages of Bresson and Ietf are not explicit about the particular way that the claimed invention, as a whole, would produce such autonomous nature of data handling. This is difficult to quote from any single phrase or any single word of the claim; the autonomous nature is difficult to quote, but prominently exists. For example, the dialog session key for encrypting a message and the dialog session key for decrypting that message or any other message can be different. Separate dialog keys permit separate fiefdoms instead of the entire kingdom of network being ruled by a single session key.

Helland teaches such autonomous nature. Mr. Helland (the person in this Helland reference) is of the same company as that of this patent application. Helland (the reference) contains a section in which Mr. Helland and Mr. Flessner discuss

fiefdom and autonomous nature (which are usually expressed in certificates and/or dialog sessions being unique).

These passage of Bresson, Ietf, Helland are not explicit about the different dialog keys being used for the same service (as in the claims).

SecureConversation teaches such different dialog keys being used for the same service (section 5. Deriving Keys, i.e., the derived key situation permits and recommends each party changing session keys and the other party being able to derive the keys needed for use in the service) for the motivation of establishing and sharing security contexts.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the teachings of Bresson, Ietf, Helland and SecureConversation for the motivations noted in the previous paragraphs so as to teach the claimed invention.

Conclusion

The art made of record and not relied upon is considered pertinent to applicant's disclosure. The art disclosed general background.

Points of Contact

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

(571) 273-8300, (for formal communications intended for entry)

Or:

(571) 273-3836 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Jung whose telephone number is (571) 272-3836 or Kambiz Zand whose telephone number is (272) 272-3811.

David Jung

Patent Examiner

8/19/07